明 細 書

ディジタル記録装置、ディジタル再生装置及びディジタル記録再生装置、並びに、暗号化装置、暗号復調装置、暗号化方法及び暗号復調方法

技術分野

[0001] この発明は、映像情報、音声情報、その他データをハードディスクや、光ディスクやメモリに記録または再生を行う、ディジタル記録装置、ディジタル記録再生装置及びディジタル記録再生装置、並びに、暗号化装置、暗号復調装置、暗号化方法及び暗号復調方法に関するものである。

背景技術

[0002] TVチューナーやビデオカメラ等からの映像信号を記録するときに、操作者は所望の時点から記録ボタンを操作するが、ディジタル記録装置の起動に所定の時間がかかるため、記録ボダンを操作してから所定の時間後に記録が開始される。この問題を回避するために起動が完了するまでメモリに一旦映像信号を記録し、起動完了後にメモリのデータを記録媒体に記録する方式がある(例えば、特許文献1参照)。

[0003] 特許文献1:特開平08−306133号公報(第2−4頁、第1ー3図)

発明の開示

発明が解決しようとする課題

[0004] 上記の方式は、暗号化が不要な信号の記録再生における起動時の対策であるが、専ら暗号化が不要なデータを対象としたものであった。

最近では著作権保護のためコンテンツ保護が必要な番組もあり、それに対しては、ディジタル記録信号を暗号化して記録媒体に記録し、また記録媒体から読み出してディジタル記録信号を復調する必要がある。現在はコンテンツ保護の必要のない番組がほとんどであるため、必要な時にだけ、暗号化回路及び暗号復調回路を作動させることができれば、省電力化につながる。その場合、特に記録または再生中に番組の変更等によりデータの暗号化または復調(暗号の解除)が必要となった場合、暗号化回路または暗号復調回路の起動に所定の時間を要するため、暗号化回路または暗号復調回路の起動時間中に番組を記録または再生できないという問題があった

。

[0005] この発明は、上記のような問題点を解決するためになされたものであり、データに暗号化または復調が必要な場合、必要でない場合に関わらず、常に要求時点から記録または再生ができるディジタル記録装置、ディジタル再生装置及びディジタル記録再生装置、並びに、暗号化装置、暗号復調装置、暗号化方法及び暗号復調方法を得ることを目的とするものである。

課題を解決するための手段

[0006] この発明は、ディジタル記録信号が入力されるデータ制御回路と、前記データ制御回路と情報伝達が可能なメモリと、前記データ制御回路と情報伝達可能で前記ディジタル記録信号を暗号化する暗号化回路と、前記データ制御回路によって制御され、前記ディジタル記録信号を記録媒体に記録する記録手段と、前記データ制御回路に前記ディジタル記録信号の伝達の制御を行わせる記録信号処理回路とを備えたディジタル記録装置において、前記ディジタル記録信号を暗号化させる必要が発生したとき、前記暗号化回路の起動を開始し、起動中は前記ディジタル記録信号を前記データ制御回路から前記メモリに移動させて蓄えておき、暗号化回路が動作可能となった時、前記メモリに蓄えられた前記ディジタル記録信号を前記データ制御回路を経由して暗号化回路に伝達して暗号化してから、前記記録手段に記録させるものである。

また、ディジタル記録信号を記録媒体から再生する再生手段と、この再生手段を制御するとともに再生されたディジタル記録信号を出力するデータ制御回路と、前記データ制御回路と情報伝達が可能な前記メモリと、前記データ制御回路と情報伝達可能で前記ディジタル記録信号を復調する暗号復調回路と、前記データ制御回路に前記ディジタル記録信号の伝達の制御を行わせる記録信号処理回路とを備えたディジタル再生装置において、暗号化されて前記記録媒体に記録された前記ディジタル記録信号を復調させて再生する必要が発生したとき、暗号復調回路を起動している間は、それ以前に前記メモリに蓄えられていた前記ディジタル記録信号を前記データ制御回路を経て出力し、暗号復調回路が動作可能となった時、前記再生手段により読み出した前記ディジタル記録信号を前記データ制御回路を経由して暗号復調回

路に伝達して復調してから出力するものである。

本発明の暗号化装置は、ディジタル信号を蓄積する蓄積手段と、前記ディジタル信号を暗号化する暗号化手段と、前記暗号化手段を有効化する暗号鍵を生成する暗号鍵生成手段と、前記ディジタル信号について前記暗号化手段により暗号化する必要があるかどうかを判断する判断手段と、前記判断手段により暗号化する必要がないと判断された場合は、前記暗号化手段による暗号化を行わずに、前記蓄積手段に蓄積されたディジタル信号を出力し、前記判断手段により暗号化する必要があると判断された場合は、当該判断の時点から前記暗号化手段が前記暗号鍵により有効化されるまでの間の前記ディジタル信号を前記蓄積手段に蓄積しておき、前記有効化が行われた後で前記暗号化手段により暗号化して出力するよう制御する制御手段とを備える。

本発明の暗号復調装置は、ディジタル信号を蓄積する蓄積手段と、前記ディジタル信号のうち暗号化された信号を暗号復調する暗号復調手段と、前記暗号復調手段を有効化する暗号鍵を生成する暗号鍵生成手段と、前記ディジタル信号について前記暗号復調手段により暗号復調する必要があるかどうかを判断する判断手段と、前記判断手段により暗号復調する必要がないと判断された場合は、前記暗号復調手段による暗号復調を行わずに、前記蓄積手段に蓄積されたディジタル信号を出力し、前記判断手段により暗号復調する必要があると判断された場合は、当該判断の時点から前記暗号復調手段が前記暗号鍵により有効化されるまでの間、前記蓄積手段にすでに蓄積されているディジタル信号を出力し、前記有効化が行われた後で前記暗号化された信号を前記暗号復調手段により暗号復調して出力するよう制御する制御手段とを備える。

また、本発明の暗号化方法は、ディジタル信号を蓄積する工程と、前記ディジタル信号を暗号化する工程と、前記暗号化を有効化する暗号鍵を生成する工程と、前記ディジタル信号について前記暗号化する必要があるかどうかを判断する工程と、前記暗号化する必要がないと判断された場合は、前記暗号化を行わずに、前記蓄積されたディジタル信号を出力し、前記暗号化する必要があると判断された場合は、当該判断の時点から前記暗号化が前記暗号鍵により有効化されるまでの間の前記ディジタ

ル信号を蓄積しておき、前記有効化が行われた後で前記暗号化して出力するよう制御する。

また、本発明の暗号復調装置は、ディジタル信号を蓄積する工程と、前記ディジタル信号のうち暗号化された信号を暗号復調する工程と、前記暗号復調を有効化する暗号鍵を生成する工程と、前記ディジタル信号について前記暗号復調する必要があるかどうかを判断する工程と、前記暗号復調する必要がないと判断された場合は、前記暗号復調を行わずに、前記蓄積されたディジタル信号を出力し、前記暗号復調する必要があると判断された場合は、当該判断の時点から前記暗号復調が前記暗号鍵により有効化されるまでの間、すでに蓄積されているディジタル信号を出力し、前記有効化が行われた後で前記暗号化された信号を前記暗号復調して出力するよう制御する。

発明の効果

[0007] 本発明のディジタル記録装置、暗号化装置及び暗号化方法は、暗号化の必要が無い番組から暗号化が必要な番組に切り替わった場合、記録を中断することなく暗号化が必要なときにだけ暗号化回路を有効化させ、暗号化の必要な番組へ切り替わってから前記記録再生手段が暗号化された信号の記録する準備ができるまでの間のデータも前記記録媒体に記録をすることができるので、暗号化の必要有無に関係なく、操作者が記録ボタンを操作した時点から記録することが出来る。

また、本発明のディジタル再生装置、暗号復調装置及び暗号復調方法は、再生中に暗号の復調が必要なデータに切り替わった場合、切り替わってから暗号復調回路を有効化するまでの間も中断することなく再生を継続することが出来る。

図面の簡単な説明

[0008] [図1]ディジタル記録装置の一実施の形態のシステム図である。

[図2]ディジタル記録装置の一実施の形態のメモリのデータの遷移を示す図である。

[図3]ディジタル再生装置の一実施の形態のシステム図である。

[図4]ディジタル再生装置の一実施の形態のメモリのデータの遷移を示す図である。

[図5]ディジタル記録再生装置の一実施の形態のシステム図である。

[図6]ディジタル記録再生装置の一実施の形態のメモリのデータの遷移を示す図であ

る。

[図7]ディジタル記録再生装置の他の実施の形態のメモリのデータの遷移を示す図である。

[図8]ディジタル記録装置の他の実施の形態のメモリのデータの遷移を示す図である。

[図9]ディジタル記録装置の他の実施の形態のシステム図である。

[図10]ディジタル再生装置の他の実施の形態のシステム図である。

[図11]ディジタル記録再生装置の他の実施の形態のシステム図である。

符号の説明

[0009] 1 MPEGエンコーダ、2a 第2のデータ制御回路、2b 第2のデータ制御回路、2c 第3のデータ制御回路、3 CPU、4 メモリ、5 暗号化回路、6 インターフェース、7 暗号鍵生成回路、8a～8c DVDドライブ、9 相互認証回路、10 暗号復調回路、11 MPEGデコーダ、12 セレクタ、13 セレクタ。

発明を実施するための最良の形態

[0010] 実施の形態1.

図1は、この発明に係わるディジタル記録装置の一実施の形態のシステム図である。MPEGエンコーダ1によって符号化されたディジタル記録信号は第1のデータ制御回路2aに入力される。第1のデータ制御回路2aは記録信号処理回路であるCPU3によって制御される。また、第1のデータ制御回路2aは、ディジタル信号を蓄積する蓄積手段であるメモリ4(蓄積手段)、ディジタル信号を暗号化する暗号化回路5及びインターフェース(I/F)6に電気的に接続されている。暗号化回路5は、暗号化回路5を有効にするために必要な暗号鍵を生成する暗号鍵生成回路7に電気的に接続されている。第1のデータ制御回路2aは、インターフェース6を介して、記録手段であるDVDドライブ8aを制御して記録媒体(図示せず)に情報を記録させることが出来る。DVDドライブ8aは記録機能と再生機能を併せ持つものであってもよい。相互認証回路9はインターフェース6と暗号鍵生成回路7に電気的に接続されており、インターフェース6を経由してDVDドライブ8aと相互認証を行う。具体的には、DVDドライブ8a側と相互認証回路9側とがお互い正規なデバイスであることを互いに確認する相互

認証を行った後、DVDドライブ8aは、インターフェース6によって他に情報が漏れて解読されないように、記録媒体個別の情報である、暗号鍵の元となる情報を当該記録媒体から読み出し、これを暗号化して相互認証回路9に送る。相互認証回路9はその暗号化された暗号鍵の元となる情報を解読し、これを暗号鍵生成回路7に伝達する。暗号鍵生成回路7は暗号鍵の元となる情報から暗号鍵を生成し、暗号化回路5に伝達する。

[0011] 以下、暗号鍵の生成について詳述する。DVDディスク等の記録媒体において、管理情報が記録されている管理情報領域には、暗号鍵の元となる情報が記録されている。暗号化すべき情報を記録媒体に記録する際は、記録媒体に記録されている暗号鍵の元となる情報から生成される暗号鍵を用いて、コンテンツ情報を暗号化して、記録される。一方、暗号化されている情報を記録媒体から再生する際は、記録媒体に記録されている暗号鍵の元となる情報から生成される暗号鍵を用いて、暗号化されている情報を復号化して、再生される。この暗号鍵の元となる情報が記録媒体から読み出されてインターフェース6を流れる時に読み出されて解読される可能性があるため、鍵転送用の暗号鍵(以下、鍵転送用のバス鍵という)により暗号化されて伝送される。この鍵転送用のバス鍵を作成するには、DVDドライブ8a側と相互認証回路9側とがお互い正規なデバイスであることを互いに確認する、相互認証を通じて行われる。DVDドライブ8aにDVDディスクが挿入されると、DVDドライブ8aは、DVDドライブ8a自身が有しているバス鍵の元(A)を相互認証回路9に送る。DVDドライブ8aと相互認証回路9とは、このバス鍵の元(A)からそれぞれ別にバス鍵(A)を計算する。相互認証回路9は計算した結果のバス鍵(A)をDVDドライブ8aに転送し、DVDドライブ8aではDVDドライブ8a自身が計算した結果と比較して、同一のバス鍵(A)が生成されていることを確認する。次に、相互認証回路8側から、DVDドライブ8aへ、相互認証回路8自身が保有しているバス鍵の元(B)が転送され、同様に計算が行われ、お互い計算したバス鍵(B)が一致していることを相互認証回路8は確認する。このようにしてバス鍵(A)とバス鍵(B)とについて一致していることが確認されると、DVDドライブ8a及び相互認証回路は、バス鍵(A)とバス鍵(B)とから、上記鍵転送用のバス鍵をそれぞれ生成する。次に、記録媒体上の暗号鍵の元となる情報から暗号鍵を

作るため、DVDドライブ8a側で記録媒体上の暗号鍵の元となる情報を鍵転送用のバス鍵で暗号化して、相互認証回路9に送る。相互認証回路9では、受け取ったデータから鍵転送用のバス鍵で暗号鍵の元となる情報を復号する。鍵生成回路7は、この暗号鍵の元となる情報から暗号鍵を生成する。この暗号鍵が暗号化回路5に伝達されることで、暗号化回路5はアクティブな状態となる。

[0012] ところで、DVD等の記録媒体においては、コピーマネージメントに関する処理を行う必要があるため、著作権の保護の必要な番組のディジタル記録信号を暗号化して記録することが義務付けられており、CGMS(Copy Generation Management System)で1回だけの記録が許されている。CGMSの信号は画像信号の一部に含まれており、CPU3によって暗号化が必要かどうか判断される。

しかし、通常の地上波で放送されるアナログの放送の番組は、CGMSによって著作権保護が必要ではない番組が大半である。このような番組を記録する場合、暗号化回路5で暗号化せずに記録媒体に記録してもよい。しかし、暗号化の必要のない番組を記録している途中から、暗号化の必要な番組に切り替わる場合は、暗号化回路5を有効化させて番組を暗号化してDVDドライブ8aによって記録媒体に記録する必要がある。

[0013] 動作について説明する。図2は、この発明に係わるディジタル記録装置の一実施の形態のメモリ4のデータの遷移を示す図である。(a)は第1のデータ制御回路2aを流れるデータを、(b)はメモリ4内の記録用の領域のデータ量Sraの変化を時系列に示している。操作者により記録媒体が機器に挿入されると、CPU3より第1のデータ制御回路2aとインターフェース6を経由してDVDドライブ8aへ起動命令が出される。DVDドライブ8aは記録媒体の回転を開始し、各種サーボの設定を行い、記録媒体を記録するために必要な情報を読み込んだ後、インターフェース6と第1のデータ制御回路2aを経由してCPU3に準備ができたことを知らせる。そして、CGMSによる著作権保護が必要ではない番組の記録要求があると、CPU3はMPEGエンコーダ1に対して、符号化してディジタル記録信号を第1のデータ制御回路2aに入力するよう指示する。MPEGエンコーダ1からは一定量の符号化が完了する度に、MPEGエンコーダ1から、第1のデータ制御回路2aを経由してメモリ4中の記録用に割り当てられた領

域にデータが転送される。このデータの転送は数百Mビット／秒以上のメモリ間での転送のため短時間で完了する。そして、第1のデータ制御回路2aを経由してインターフェース6から、DVDドライブ8aの記録媒体へと記録が開始される。DVDドライブ8aでの記録媒体への書き込み速度は、数十Mビット／秒程度であるためメモリ4へ転送の数倍の時間を要する。

[0014] 記録している番組が、途中の時刻T4で暗号化が必要な番組に切り替わるとき、CPU3はCGMSによって暗号化が必要であることを判断し、メモリ4からのデータの読み出しおよび記録媒体への記録を一時停止するよう、第1のデータ制御回路2aを経由してインターフエース6に指示する。しかしMPEGエンコーダ1の符号化は停止させないため、メモリ4の記録用に割り当てられた領域へのディジタル記録信号のデータの蓄積は継続される。このときメモリ4の記録用の領域の空き容量は暗号化回路5を有効にするまでの時間、オーバーフローを防止するため、メモリ4内の記録用の領域のデータ量はSr3以下を確保する必要がある。確保できていない場合は、メモリ4から記録媒体への記録動作を継続し、十分な空き容量が確保された段階で、記録媒体への書き込みを停止する。

[0015] 暗号化する必要があると判断された当該判断時点から暗号化回路5が暗号鍵により有効化されるまでの間、上述したように、DVDドライブ8a側と相互認証回路9側とが相互認証を行い、記録媒体から暗号鍵の元となる情報を読み出し、暗号鍵生成回路7はこれから暗号鍵を生成して、暗号化回路5は暗号鍵によって有効化される。

暗号化回路5が有効になることでDVDドライブ8aの暗号化記録が可能となる。時刻T5で暗号化回路5が有効になると、メモリ4に蓄積されたデータは、第1のデータ制御回路2aを経由して、暗号化回路5で暗号化され、再び第1のデータ制御回路2aを経由して、メモリ4の書き込み用に割り当てられた領域に戻される。さらにDVDドライブ8aで書き込み可能な記録レートで、メモリ4の書き込み用に割り当てられた領域から第1のデータ制御回路2aを経由してインターフェース6へ出力され、DVDドライブ8aで記録媒体への記録が再開される。但し、この時点ではメモリ4内に暗号化の必要のない番組のデータが残っているため、暗号化の必要のないデータは暗号化を行わない。

[0016] このとき、MPEGエンコーダ1で符号化されるビットレートをxMビット／秒、暗号化が必要な番組に切り替わった時点T4でのメモリ4のデータ量はSr3以下であり、メモリ4中の記録用の領域の容量をC1とすると、C1≧x×(T5−T4)＋Sr3を満たせばよい。即ち、暗号化が必要であると判断された場合は、当該判断の時点T4でのメモリ4のデータ量Sr3は、上記式を満たすようなデータ量に制御しておく必要がある。逆に言えば、メモリ4の空き容量は、暗号化が必要であると判断された判断の時点から暗号化回路5が暗号鍵により有効化されるまでの間のディジタル信号を蓄積可能な容量以上である必要がある。

なお、暗号化が必要であると判断された当該判断の時点T4において、メモリ4のデータ量Sr3が確保できていない場合は、メモリ4から暗号化の必要のないデータを記録媒体へ記録する動作を継続し、十分な空き容量が確保された段階で、記録媒体への書き込みを停止するため、厳密に言えば、確保すべきメモリ4のデータ量Sr3は、上記T4の時点のものである必要はなく、T4の時点より後であって記録動作を停止した時点のものでよい。

[0017] メモリ4の書き込み用に割り当てられている領域の容量は、すぐにDVDドライブ8aに記録されるため、数kー数十kバイト程度で十分である。

[0018] 従って、DVDドライブ8aの記録中に暗号化の必要な番組に切り替わった場合、CPU3による暗号化の必要があるとの判断の時点から、暗号化回路5が暗号鍵により有効化されるまでの間のディジタル信号をメモリ4に蓄積しておき、暗号化回路5が有効となった後に暗号化してDVDドライブ8aに記録することが出来るので、記録データの暗号化が必要な場合、必要でない場合に関わらず、常に要求時点から、書き込み型光ディスク、書換え可能型光ディスク等の記録媒体に記録することが可能である。

[0019] 実施の形態2.

図3は、この発明に係わるディジタル再生装置の一実施の形態のシステム図である。実施の形態2において、実施の形態1と比べて第1のデータ制御回路2aの代わりにディジタル記録信号が出力可能な第2のデータ制御回路2bが備えられ、DVDドライブ8aの代わりのDVDドライブ8bは再生専用であり、暗号化回路5の代わりに、暗号

復調回路10が暗号鍵生成回路7と第2のデータ制御回路2bに電気的に接続されている。暗号復調回路10は暗号化回路5と同様に暗号鍵生成回路7からの暗号鍵の伝達を受けると有効となり、暗号化されたディジタル記録信号を復調することが出来る。また、実施の形態1におけるMEPGエンコーダ1に代えてMPEGデコーダ11が第2のデータ制御回路2bと電気的に接続されており、ディジタル記録信号は、第2のデータ制御回路2bを経由してMPEGデコーダ11によって復号化される。DVDドライブ8bは記録機能と再生機能とを併せ持つものであってもよい。

[0020] 動作について説明する。図4は、この発明に係わるディジタル再生装置の一実施の形態のメモリ4のデータの遷移を示す図である。(a)は第2のデータ制御回路2bを流れるデータを、(b)はメモリ4内の読み出し用の領域のデータ量Srbの変化を時系列に示している。記録媒体からデータを読み出し中に、ディジタル記録信号が暗号化されていないものから暗号化されたものに切り替わった場合の動作を説明する。

DVDドライブ8bにより記録媒体から暗号化されていないデータを読み出す際には、DVDドライブ8bの記録媒体のデータはインターフェース6と第2のデータ制御回路2bを経由してメモリ4の読み出し用に割り当てられた領域に記録される。その際、このデータは暗号化されてないデータであるとCPU3によって判別されるので、その後はメモリ4から第2のデータ制御回路2bを経由してMPEGデコーダ11に出力される。

[0021] 時刻T6に暗号を復調することが必要な番組であるとCPU3が認識すると、CPU3は、DVDドライブ8bからメモリ4へのデータの読み出しを一時停止するよう、第2のデータ制御回路2bを経由してインターフエース6に指示する。しかしMPEGデコーダ11により復号した映像は再生中であり、ディスプレイでの映像を停止させないため、メモリ4からMPEGデコーダ11へのディジタル記録信号の排出は継続される。このときメモリ4内の読み出し用の領域の容量は暗号復調回路10を有効にするまでの時間はディジタル記録信号を排出し続けるため、メモリ4内の読み出し用の領域のデータ量はSr4以上を確保する必要がある。時刻T6からT7の間にMPEGデコーダ11へ連続して出力されるべきデータ量をΔPとすると、ΔP≦Sr4の関係がある。即ち、暗号復調する必要があると判断された場合は、当該判断の時点T6でのメモリ4のデータ量Sr4は、上記式を満たすような、当該判断の時点T6から暗号復調回路10が暗号

鍵により有効化されるまでの間に出力されるデータ量以上に制御しておく必要がある。Sr4がΔP以下であると暗号復調回路10を有効化する間にメモリ4内の読み出し用の領域のディジタル記録信号のデータ量が0となり、再生できなくなるからである。ここで、暗号復調回路10が暗号鍵により有効化されるまでの間出力されるディジタル信号は、暗号復調する必要のない信号である。

[0022] 記録媒体からの読み出しが停止している間に、DVDドライブ8bと相互認証回路9とは相互認証を行った後、DVDドライブ8bから暗号鍵の元となる情報を読み出し、暗号鍵生成回路7にて暗号鍵の生成を行い、暗号復調回路10が暗号鍵によって有効となる。時刻T7に暗号復調回路10が有効になると、その後にDVDドライブ8bから読み出されたデータは、一旦メモリ4の読み出し用に割り当てられた領域に蓄積された後、第2のデータ制御回路2bを経由して、暗号復調回路10で復調され、再び第2のデータ制御回路2bを経由して、一旦メモリ4の再生用に割り当てられた領域に格納される。その後復調されたディジタル記録信号はMPEGデコーダ11によって復号され、出力される。

[0023] 従って、DVDドライブ8bから読み出し中に暗号を復調することが必要な番組に切り替わった場合でも、CPU3による暗号復調する必要があるとの判断の時点から、暗号復調回路10が暗号鍵により有効化されるまでの間、メモリ4にすでに蓄積されているディジタル信号を出力し、暗号復調回路10が有効となった後、DVDドライブ8bから読み出したデータを復調して出力することが出来るので、記録データの復調が必要な場合、必要でない場合に関わらず、常に要求時点から、再生専用光ディスク等の記録媒体から再生することが可能である。

[0024] 実施の形態3.

近年DVDドライブの記録・再生ビットレートが向上しており、同一ディスクに対して記録と再生を同時に行うことができるようになっている。これには現在記録中の番組を再生する場合と、現在記録している番組とは異なる番組を再生する場合とがある。記録している番組とは異なる番組を再生する場合、先に暗号化する必要のない番組の記録を開始し、後から暗号化された番組の再生を行う場合が考えられる。

[0025] 図5は、この発明に係わるディジタル記録再生装置の一実施の形態のシステム図で

ある。実施の形態1の場合と比べて、第1のデータ制御回路2aはディジタル記録信号が入出力可能で、第1のデータ制御回路2aと第2のデータ制御回路2bの双方の機能を併せ持つ第3のデータ制御回路2cに置き換えられ、DVDドライブ8aは記録再生可能なDVDドライブ8cに置き換えられている。実施の形態1の場合に加えて、暗号復調回路10は暗号鍵生成回路7と第3のデータ制御回路2cに電気的に接続されている。暗号復調回路10は暗号化回路5と同様に暗号鍵生成回路7からの暗号鍵の伝達を受けると、有効となり、暗号化されたディジタル記録信号を解除することが出来る。また、ディジタル記録信号は、第3のデータ制御回路2cを経由してMPEGデコーダ11によって復号される。その他は、実施の形態1，2と同様である。

[0026] 動作について説明する。図6は、この発明に係わるディジタル記録再生装置の一実施の形態のメモリ4のデータの遷移を示す図である。(a)は第3のデータ制御回路2cを流れるデータ、(b)はメモリ4内の記録用の領域のデータ量Sraと、読み出し用の領域のデータ量Srbの変化を時系列に示している。

[0027] 時刻T8以前においては、暗号化の必要のない番組を記録している。時刻T8において、記録媒体に記録されている暗号化された番組の再生要求が出されると、CPU3はDVDドライブ8cへのディジタル記録信号の転送の中断を第3のデータ制御回路2cに指示する。この時録画されるべきディジタル記録信号の流れは継続されているため、MPEGエンコーダ1から符号化されたディジタル記録信号のデータは、記録が中断される前と同様にメモリ4の記録用に割り当てられた領域へ蓄積され続ける。

[0028] この間に暗号復調回路10を有効にするため、DVDドライブ8cと相互認証回路9とは相互認証を行った後、暗号鍵の元となる情報を記録媒体から読み出して、鍵生成回路7において暗号鍵の生成が行われる。生成された暗号鍵により暗号復調回路10を有効にした後、時刻T9よりDVDドライブ8cは記録媒体からのデータの読み出しを開始し、読み出されたデータは第3のデータ制御回路2cを経由してメモリ4の読み出し用に割り当てられた領域に一旦格納され、再び第3のデータ制御回路2cを経由して、暗号復調回路10に送られる。暗号復調回路10で暗号が解除されたデータは再び第3のデータ制御回路2cを経由してメモリ4の再生用に割り当てられた領域へ蓄積される。さらに所定の量が蓄積されると、符号化されたデータを復号するMPEG

デコーダ11へと転送される。

[0029] 暗号復調回路10が有効になった時刻T9以降、時刻T10にメモリ4の記録用に割り当てられた領域のデータ量Sraが所定の量Sr5を超えると、蓄積されたデータは第3のデータ制御回路2cを経由してインターフェース6へ転送され、DVDドライブ8cの記録媒体への書き込みを再開する。

[0030] このとき、DVDドライブ8cへのデータ転送を一時停止する直前のメモリ4に残っている記録用の符号化されたデータ量SraをSr10とし、MPEGエンコーダ1で符号化されるビットレートをx、再生を開始してから次にDVDドライブ8cが記録を行うまでの時間を(T10−T8)、メモリ4中の記録用に割り当てられている容量をC2とするとC2＞Sr10＋x×(T10−T8)を満たすようする必要がある。

この後、DVDドライブ8cは一定量の読み出し後、メモリ4の記録用に割り当てられた領域のデータ量Sraが所定の量Sr5を超えるごとに記録媒体への書き込みを行い、またメモリ4の再生用に割り当てられた領域のデータ量SrbがSr11を下回るごとに記録媒体からの読み出しを行う。

[0031] 従って、DVDドライブ8cが暗号化の必要のない番組を記録中に暗号化の必要な番組の再生が要求された場合でも、暗号復調回路10の有効化している間、記録用ディジタル信号をメモリ4に保存し、暗号復調回路10が有効となった後、DVDドライブ8cから読み出したデータの暗号を復調して再生し、同時にDVDドライブ8c内の記録媒体に記録することが出来るので、記録データの暗号化が必要な場合、必要でない場合に関わらず、記録媒体に記録中であっても常に要求時点から再生することが可能である。

[0032] 実施の形態4.

実施の形態3では暗号化する必要のない番組を記録している最中に、暗号復調回路10を有効にして、暗号化された番組を再生する場合について述べたが、暗号化されていない番組の再生をしている最中に、暗号化回路5を有効にして記録を行う場合について以下述べる。この実施の形態のディジタル記録再生装置の構成は実施の形態3の図5と同じである。

[0033] 動作について説明する。図7は、この発明に係わるディジタル記録再生装置の他の

実施の形態のメモリ4のデータの遷移を示す図である。(a)は第3のデータ制御回路2cを流れるデータ、(b)はメモリ4の記録用のデータ量Sraと、再生用のデータ量Srbの変化を時系列に示している。

暗号化されていない番組を再生している最中に、時刻T11に記録要求が出されると、CPU3はMPEGエンコーダ1の符号化を開始させ、メモリ4の記録用に割り当てられた領域へのデータ転送を開始する。暗号化回路5を有効化している間は、記録媒体からの再生を行うことができないため、メモリ4内の再生用に割り当てられた領域に、ディスプレイでの映像の再生を継続するのに十分なデータ量Sr6が蓄積された時刻T12a以降に暗号化回路5の有効化を開始する。DVDドライブ8cと相互認証回路9とで相互認証を行った後、記録媒体に記録されている暗号鍵の元となる情報から鍵生成回路7で暗号鍵を生成し、この暗号鍵をもとに暗号化回路5を時刻T12bにおいて有効にする。

[0034] 暗号化回路5を有効化している間も、録画用のデータの流れとディスプレイでの映像の再生は継続する必要があるため、メモリ4中の記録用に割り当てられた領域へMPEGエンコーダ1で符号化されたディジタル記録信号のメモリ4への書き込みは継続される。また、メモリ4内の読み出し用に割り当てられた領域にあるデータは、MPEGデコーダ11へ供給され続ける。暗号化回路5が有効となった時刻T12b以降で、記録用に割り当てられた領域のデータ量が時刻T13に所定の容量Sr7を超えると、蓄積されたデータは第3のデータ制御回路2cを経由して暗号化回路5で暗号化される。さらに第3のデータ制御回路2cを経由して、メモリ4内の書き込み用に割り当てられた領域へもう一度格納された後、再び第3のデータ制御回路2cを経由してインターフェース6へ転送され、DVDドライブ8cで記録媒体への書き込みが開始される。記録媒体への書き込みは、記録用のデータ量がSr8に減少するまで続けられる。更に時刻T14で、再生用に割り当てられた領域のデータ量がSr9を下回るとDVDドライブ8による記録媒体からの読み出しを再開する。

[0035] 先ほども述べたように、暗号化回路5を有効化している間、およびメモリ4の記録用に割り当てられて領域に蓄積されたデータが、記録媒体に書き込まれるまでの間は、記録媒体からの再生を行うことができない。そのためメモリ4内の、再生用に割り当て

られた領域に、これらの間ディスプレイでの映像の再生を継続できるに十分なデータ量Sr6を蓄積してから、暗号化回路5の有効化を行う必要がある。ここで蓄積しておく必要のあるデータ量Sr6は、再生データの符号化ビットレートをyMbpsとすると、Sr6＞(T14−T12a)・yを満たす必要がある。

[0036] また、メモリ4内の記録用に割り当てられた領域で、最低限確保する必要のある容量をC3、記憶媒体への記録を再開する時刻をT13とすると、C3＞(T13−T11)×xを満たす必要がある。

[0037] 従って、DVDドライブ8cが暗号化の必要のない番組を再生中に暗号化の必要な番組の記録が要求された場合でも、暗号化回路5の有効化している間、記録用ディジタル信号をメモリ4に保存し、暗号化回路5が有効となった後、暗号化してDVDドライブ8cにデータを記録し、同時にDVDドライブ8c内の記録媒体のデータを再生すること出来るので、記録データの暗号化が必要な場合、必要でない場合に関わらず、常に要求時点から、記録媒体からに記録及び再生することが可能である。

[0038] 実施の形態5.

実施の形態1において、操作者により記録媒体が機器に挿入された後すぐに記録要求があった場合は、DVDドライブ8aを起動させるのにある程度の時間を要するが、DVDドライブ8aが初期起動中に著作権保護の必要な番組の記録要求がある場合があり、この場合について説明する。

実施の形態5におけるデジタル記録装置は実施の形態1と同じであり、図1に示されたものと同じである。

[0039] 動作について説明する。図8は、この発明に係わるディジタル記録装置の他の実施の形態のメモリのデータの遷移を示す図である。(a)は第1のデータ制御回路2aを流れるデータを示し、(b)はメモリ4内の記録用の領域のデータ量Sraの変化を時系列に示している。

操作者により記録媒体が機器に挿入されると、CPU3より第1のデータ制御回路2aとインターフェース6を経由してDVDドライブ8aへ起動命令が出される。DVDドライブ8aは記録媒体の回転を開始し、各種サーボの設定を行い、記録媒体を記録・再生するために必要な情報を読み込んだ後、インターフェース6と第1のデータ制御回路

2aを経由してCPU3に準備ができたことを知らせる。上記の動作を行っている最中に操作者により、時刻T1に暗号化が必要なデータの記録が要求されると、CPU3はMPEGエンコーダ1に対して、符号化してディジタル記録信号を第1のデータ制御回路2aに入力するよう指示する。その際にCPU3はCGMSによって暗号化が必要であることを判断する。一定量の符号化がMPEGエンコーダ1により完了する度に、MPEGエンコーダ1から、第1のデータ制御回路2aを経由してメモリ4中の記録用に割り当てられた領域にデータが転送される。このデータの転送は数百Mビット／秒以上のメモリ間での転送のため短時間で完了する。以後、MPEGエンコーダ1によってエンコードされたデータはDVDドライブ8aの記録準備が完了するまで、メモリ4中へ符号化されたデータが蓄積され続ける。

[0040] DVDドライブ8aの起動が時刻T2aに完了すると暗号化回路5の有効化が開始され、時刻T2bに完了する。これによりDVDドライブ8aの暗号化記録も可能となる。その間も、メモリ4中へ符号化されたデータが蓄積され続ける。

[0041] DVDドライブ8aの記録準備が完了する時刻T2b以降で、メモリ4中の記録用に割り当てられた領域のデータ量が一定量Sr1以上蓄積されると、第1のデータ制御回路2aを経由して、暗号化回路5で暗号化され、再び第1のデータ制御回路2aを経由してメモリ4中の書き込み用に割り当てられた領域へ戻され、すぐに第1のデータ制御回路2aを経由してインターフェース6から、DVDドライブ8aの記録媒体へと記録が開始される。記録媒体への記録は、メモリ4の記録用に割り当てられた領域が所定の容量Sr2以下になるまで、インターフェース6からDVDドライブ8aを経て行われる。DVDドライブ8aでの記録媒体への書き込み速度は、数十Mビット／秒程度であるためメモリ4へ転送の数倍の時間を要する。MPEGエンコーダ1で符号化されるビットレートをxMビット／秒、光磁気ディスクへの書き込みが始まる時間をT3とすると、最低限必要なメモリ4中の記録用の領域の容量C4との関係は$C4 > x \times (T3-T1)$を満たす必要がある。また、暗号化回路5から一旦メモリ4を経由する際のメモリ4に割り当てられている容量は、すぐにDVDドライブ8aに記録されるために、数k一数十kバイト程度で十分である。

[0042] DVDドライブ8aが記録可能になった後も、MPEGエンコーダ1から符号化された

ディジタル記録信号の出力は継続されるが、記録媒体への書き込まれる速度の方が早いため、図8に示すようにメモリ4がオーバーフローすることはない。再びメモリ4の記録用に割り当てられた領域が、所定の容量に達するまで記録媒体への書き込みは行わず、所定の容量を超える度に、まとめてデータが書き込まれる。

[0043] 従って、DVDドライブ8aの起動中に暗号化の必要な番組の記録要求があった場合でも、DVDドライブ8aの起動及び暗号化回路5の有効化している間、メモリ4に保存し、暗号化回路5が有効となった後、暗号化してDVDドライブ8aに記録することが出来るので、暗号化が必要な番組に対しても、記録を要求した時点からの記録が可能となる。

[0044] 実施の形態6.

実施の形態1及び5において、図1に示されたシステム図とは別の構成とした場合でも同様の機能及び効果を発揮することができるので、その場合について説明する。

図9は、この発明に係わるディジタル記録装置の他の実施の形態のシステム図である。実施の形態1の図1に示されたシステム図との違いは第1のデータ制御回路2aから暗号化回路5は双方向に情報伝達が可能であったが、実施の形態6においては、第1のデータ制御回路2aから暗号化回路5へのみ情報伝達することができる。また、第1のデータ制御回路2aと暗号化回路5は共にセレクタ12へ情報を伝達することができる。セレクタ12は、第1のデータ制御回路2aからのデータか暗号化回路5からのデータを選択して、インターフェース6に情報を伝達することができる。

また、第1のデータ制御回路2aからインターフェース6へは符号化されたデータ以外のデータ等が常に出力されているため、暗号化されたデータをセレクタ12なしに、暗号化されていないデータの情報伝達用の線と合流させてしまうと、データ同士がぶつかりあい、回路が壊れてしまう。よって暗号化されていないデータの情報伝達用の線との合流地点にセレクタ12は設けられている。

[0045] 動作について説明する。基本的に実施の形態1及び5と同じであるが、相違する部分について説明する。

暗号化する必要のない番組のとき、実施の形態1の場合、暗号化されていないデータはメモリ4から第1のデータ制御回路2aを経由してインターフェース6にデータが

転送されるのに対し、実施の形態6の場合、暗号化されていないデータはメモリ4から第1のデータ制御回路2aを経由して一端セレクタ12に転送され、セレクタ12が暗号化されていないデータを選択した後、インターフェース6に転送される。また、暗号化する必要のある番組のとき、実施の形態1の場合、暗号化回路5で暗号化された後は、暗号化されたデータは第1のデータ制御回路2aを経由してメモリ4の書き込み用に割り当てられた領域に戻され、さらに第1のデータ制御回路2aを経由してインターフェース6へ出力されるのに対し、実施の形態6の場合、暗号化回路5で暗号化された後は、暗号化されたデータは一端セレクタ12に転送され、セレクタ12が暗号化されたデータを選択した後、インターフェース6に転送される。

[0046] 従って、暗号化回路5で暗号化された後は、第1のデータ制御回路2aを経由してメモリ4の書き込み用に割り当てられた領域に戻されることがないので、メモリ4の書き込み用の領域を確保する必要がなくなる。また、第1のデータ制御回路2aを単位当たりに追加するデータ量が少なくなるため、実施の形態1及び5の場合よりもデータ転送速度を遅くすることが出来、システムの小型化、さらなる省電力化を図ることができる。

[0047] 実施の形態7.

実施の形態2において、図3に示されたシステム図とは別の構成とした場合でも同様の機能及び効果を発揮することができるので、その場合について説明する。

図10は、この発明に係わるディジタル再生装置の他の実施の形態のシステム図である。実施の形態2の図3に示されたシステム図との違いは第2のデータ制御回路2bから暗号復調回路10は双方向に情報伝達が可能であったが、実施の形態7においては、第2のデータ制御回路2bから暗号復調回路10へのみ情報伝達することができる。また、第2のデータ制御回路2bと暗号復調回路10は共にセレクタ13へ情報を伝達することができる。セレクタ13は、第2のデータ制御回路2bからのデータか暗号復調回路10からのデータかを選択して、MEPGデコーダ11に情報を伝達することができる。

また、第2のデータ制御回路2bからMEPGデコーダ11は符号化されたデータ以外のデータ等が常に出力されているため、復調されたデータをセレクタ13なしに、復調されていないデータの情報伝達用の線と合流させてしまうと、データ同士がぶつかり

あい、回路が壊れてしまう。よって復調されていないデータの情報伝達用の線との合流地点にセレクタ13は設けられている。

[0048] 動作について説明する。基本的に実施の形態2と同じであるが、相違する部分について説明する。

復調する必要のない番組のとき、実施の形態2の場合、復調する必要のないデータはメモリ4から第2のデータ制御回路2bを経由してMEPGデコーダ11にデータが転送されるのに対し、実施の形態7の場合、復調する必要のないデータは第2のデータ制御回路2bから一端セレクタ13へ転送され、セレクタ13が復調する必要のないデータを選択した後、MEPGデコーダ11に転送される。また、復調する必要のある番組のとき、実施の形態2の場合、暗号復調回路10で復調された後は、第2のデータ制御回路2bを経由してメモリ4の再生用に割り当てられた領域に戻され、さらに第2のデータ制御回路2bを経由してMEPGデコーダ11へ出力されるのに対し、実施の形態7の場合、暗号復調回路10で暗号化された後は、復調されたデータは、セレクタ13へ転送され、セレクタ13が復調されたデータを選択した後、MEPGデコーダ11に転送される。

[0049] 従って、暗号復調回路10で暗号化された後は、第2データ制御回路2b経由してメモリ4の再生用に割り当てられた領域に戻されることがないので、メモリ4の再生用の領域を確保する必要がなくなる。また、第2のデータ制御回路2bを単位当たりに追加するデータ量が少なくなるため、実施の形態2の場合よりもデータ転送速度を遅くすることが出来、システムの小型化、さらなる省電力化を図ることができる。

[0050] 実施の形態8.

実施の形態3及び4において、図5に示されたシステム図とは別の構成とした場合でも同様の機能及び効果を発揮することができるので、その場合について説明する。

図11は、この発明に係わるディジタル記録再生装置の他の実施の形態のシステム図である。実施の形態3の図5に示されたシステム図との違いについて説明する。

記録する側は、第3のデータ制御回路2cから暗号化回路5は双方向に情報伝達が可能であったが、実施の形態8においては、第2のデータ制御回路2cから暗号化回路5へのみ情報伝達することができる。また、第3のデータ制御回路2cと暗号化回路

5は共にセレクタ12へ情報を伝達することができる。セレクタ12は、第1のデータ制御回路2aからのデータか暗号化回路5からのデータを選択して、インターフェース6に情報を伝達することができる。

再生する側は、第3のデータ制御回路2cから暗号復調回路10は双方向に情報伝達が可能であったが、実施の形態8においては、第3のデータ制御回路2cから暗号復調回路10へのみ情報伝達することができる。また、第3のデータ制御回路2cと暗号復調回路10は共にセレクタ13へ情報を伝達することができる。セレクタ13は、第3のデータ制御回路2cからのデータか暗号復調回路10からのデータを選択して、MEPGデコーダ11に情報を伝達することができる。

[0051] 動作について説明する。基本的に実施の形態3及び4と同じであり、相違する部分については、記録する場合は実施の形態6と同じであり、再生する場合は実施の形態7と同じである。

[0052] 従って、暗号化回路5で暗号化された後は、第3のデータ制御回路2cを経由してメモリ4の書き込み用に割り当てられた領域に戻されることがないので、メモリ4の書き込み用の領域を確保する必要がなくなる。また、第3のデータ制御回路2aを単位当たりに追加するデータ量が少なくなるため、実施の形態3及び4の場合よりもデータ転送速度を遅くすることが出来、システムの小型化、さらなる省電力化を図ることができる。

また、暗号復調回路10で暗号化された後は、第3データ制御回路2c経由してメモリ4の再生用に割り当てられた領域に戻されることがないので、メモリ4の再生用の領域を確保する必要がなくなる。また、第3のデータ制御回路2cを単位当たりに追加するデータ量が少なくなるため、実施の形態3及び4の場合よりもデータ転送速度を遅くすることが出来、システムの小型化、さらなる省電力化を図ることができる。

[0053] 尚、実施の形態1乃至8では、DVDドライブ8a～8cと相互認証回路9との間で、相互認証を行うことを前提に説明をしているが、両者がローカルなインターフェースで接続されている場合や、LSIの統合化が進んでDVDドライブ8a～8c側のLSIと信号処理側のLSIが一体化された場合などは、相互認証を行う必要はなく、この場合、相互認証回路9は不要となる。また、データの符号化、復号化にMPEGエンコーダ1及びMPEGデコーダ11を使用した場合について説明したが、他の方式のエンコーダ及

びデコーダでもよく、符号化を必要としなければエンコーダ及びデコーダは無くてもよい。

[0054] 更に、実施の形態1乃至8では、DVDレコーダ(記録装置)又はDVDプレーヤ(再生装置)についての説明をしているが、ハードディスク、半導体メモリを用いた記録装置や再生装置を用いた場合についても適用することができるものである。

産業上の利用可能性

[0055] 本発明のディジタル記録装置、ディジタル再生装置及びディジタル記録再生装置、並びに、暗号化装置、暗号復調装置、暗号化方法及び暗号復調方法によれば、データに暗号化または暗号復調化が必要な場合、必要でない場合に関わらず、常に要求時点から記録または再生をスムーズに行うことができる。

請求の範囲

[1] ディジタル記録信号が入力されるデータ制御回路と、前記データ制御回路と情報伝達が可能なメモリと、前記データ制御回路と情報伝達可能で前記ディジタル記録信号を暗号化する暗号化回路と、前記データ制御回路によって制御され、前記ディジタル記録信号を記録媒体に記録する記録手段と、前記データ制御回路に前記ディジタル記録信号の伝達の制御を行わせる記録信号処理回路とを備えたディジタル記録装置において、前記ディジタル記録信号を暗号化させる必要が発生したとき、前記暗号化回路の起動を開始し、起動中は前記ディジタル記録信号を前記データ制御回路から前記メモリに移動させて蓄えておき、暗号化回路が動作可能となった時、前記メモリに蓄えられた前記ディジタル記録信号を前記データ制御回路を経由して暗号化回路に伝達して暗号化してから、前記記録手段に記録させることを特徴とするディジタル記録装置。

[2] ディジタル記録信号を記録媒体から再生する再生手段と、この再生手段を制御するとともに再生されたディジタル記録信号を出力するデータ制御回路と、前記データ制御回路と情報伝達が可能な前記メモリと、前記データ制御回路と情報伝達可能で前記ディジタル記録信号を復調する暗号復調回路と、前記データ制御回路に前記ディジタル記録信号の伝達の制御を行わせる記録信号処理回路とを備えたディジタル再生装置において、暗号化されて前記記録媒体に記録された前記ディジタル記録信号を復調させて再生する必要が発生したとき、暗号復調回路を起動している間は、それ以前に前記メモリに蓄えられていた前記ディジタル記録信号を前記データ制御回路を経て出力し、暗号復調回路が動作可能となった時、前記再生手段により読み出した前記ディジタル記録信号を前記データ制御回路を経由して暗号復調回路に伝達して復調してから出力することを特徴とするディジタル再生装置。

[3] 請求項1に記載のディジタル記録装置と請求項2に記載のディジタル再生装置を備えたことを特徴とするディジタル記録再生装置。

[4] ディジタル信号を蓄積する蓄積手段と、

前記ディジタル信号を暗号化する暗号化手段と、

前記暗号化手段を有効化する暗号鍵を生成する暗号鍵生成手段と、

前記ディジタル信号について前記暗号化手段により暗号化する必要があるかどうかを判断する判断手段と、

前記判断手段により暗号化する必要がないと判断された場合は、前記暗号化手段による暗号化を行わずに、前記蓄積手段に蓄積されたディジタル信号を出力し、

前記判断手段により暗号化する必要があると判断された場合は、当該判断の時点から前記暗号化手段が前記暗号鍵により有効化されるまでの間の前記ディジタル信号を前記蓄積手段に蓄積しておき、前記有効化が行われた後で前記暗号化手段により暗号化して出力するよう制御する制御手段とを備えることを特徴とする暗号化装置。

[5] 前記暗号鍵は、ディジタル信号を記録するための記録媒体から読み取られた情報から生成されることを特徴とする請求項4記載の暗号化装置。

[6] 前記判断手段により暗号化する必要があると判断された場合、前記蓄積手段の空き容量は、当該判断の時点から前記暗号化手段が前記暗号鍵により有効化されるまでの間の前記ディジタル信号を蓄積可能な容量以上は確保していることを特徴とする請求項4又は5記載の暗号化装置。

[7] ディジタル信号を蓄積する蓄積手段と、

前記ディジタル信号のうち暗号化された信号を暗号復調する暗号復調手段と、

前記暗号復調手段を有効化する暗号鍵を生成する暗号鍵生成手段と、

前記ディジタル信号について前記暗号復調手段により暗号復調する必要があるかどうかを判断する判断手段と、

前記判断手段により暗号復調する必要がないと判断された場合は、前記暗号復調手段による暗号復調を行わずに、前記蓄積手段に蓄積されたディジタル信号を出力し、

前記判断手段により暗号復調する必要があると判断された場合は、当該判断の時点から前記暗号復調手段が前記暗号鍵により有効化されるまでの間、前記蓄積手段にすでに蓄積されているディジタル信号を出力し、前記有効化が行われた後で前記暗号化された信号を前記暗号復調手段により暗号復調して出力するよう制御する制御手段とを備えることを特徴とする暗号復調装置。

[8] 前記暗号鍵は、ディジタル信号を記録するための記録媒体から読み取られた情報から生成されることを特徴とする請求項7記載の暗号復調装置。

[9] 前記判断手段により暗号復調する必要があると判断された場合、前記蓄積手段にすでに蓄積されているディジタル信号のデータ量は、当該判断の時点から前記暗号復調手段が前記暗号鍵により有効化されるまでの間に出力されるデータ量以上は確保していることを特徴とする請求項7又は8記載の暗号復調装置。

[10] ディジタル信号を蓄積する工程と、

前記ディジタル信号を暗号化する工程と、

前記暗号化を有効化する暗号鍵を生成する工程と、

前記ディジタル信号について前記暗号化する必要があるかどうかを判断する工程と、

前記暗号化する必要がないと判断された場合は、前記暗号化を行わずに、前記蓄積されたディジタル信号を出力し、

前記暗号化する必要があると判断された場合は、当該判断の時点から前記暗号化が前記暗号鍵により有効化されるまでの間の前記ディジタル信号を蓄積しておき、前記有効化が行われた後で前記暗号化して出力するよう制御することを特徴とする暗号化方法。

[11] ディジタル信号を蓄積する工程と、

前記ディジタル信号のうち暗号化された信号を暗号復調する工程と、

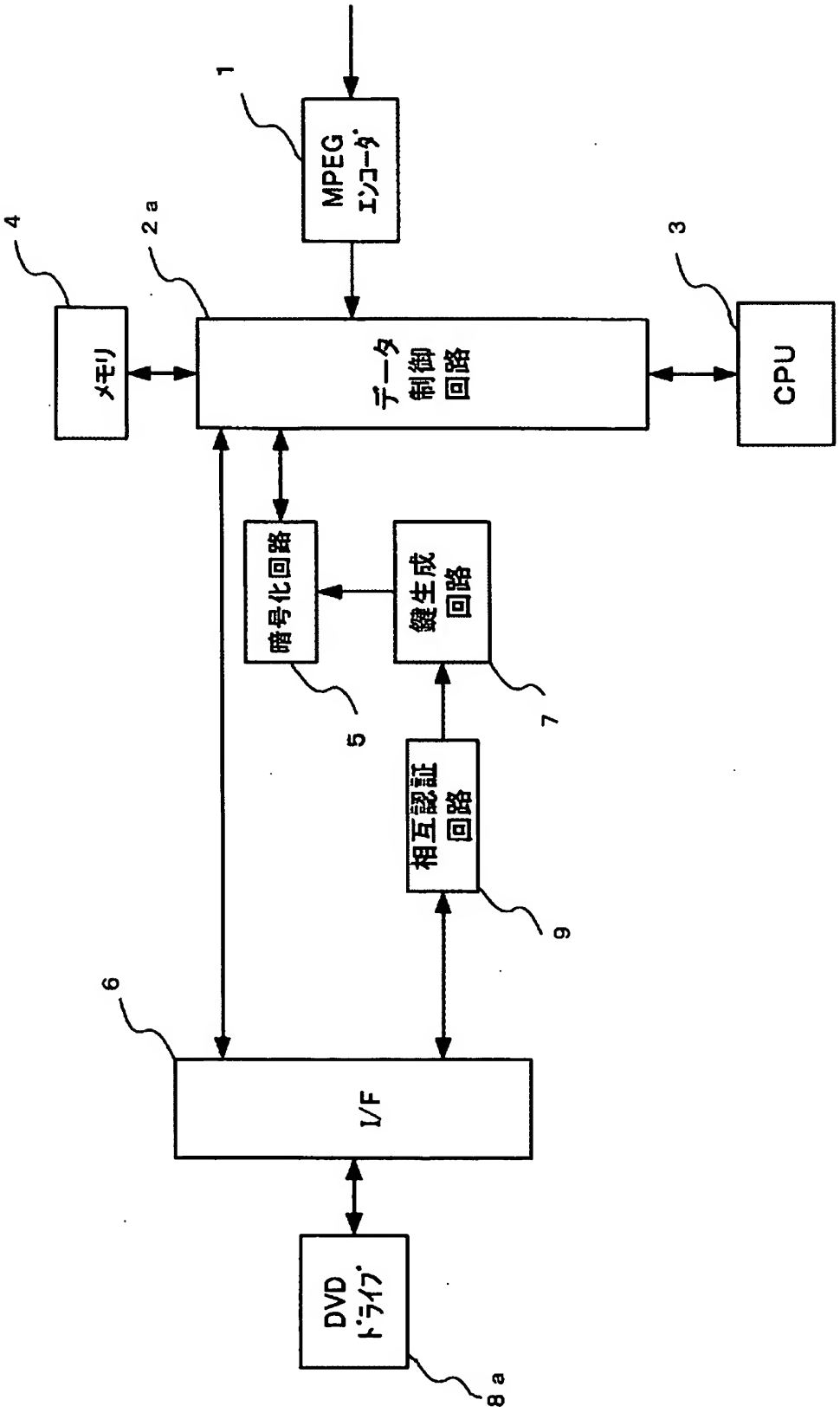
前記暗号復調を有効化する暗号鍵を生成する工程と、

前記ディジタル信号について前記暗号復調する必要があるかどうかを判断する工程と、

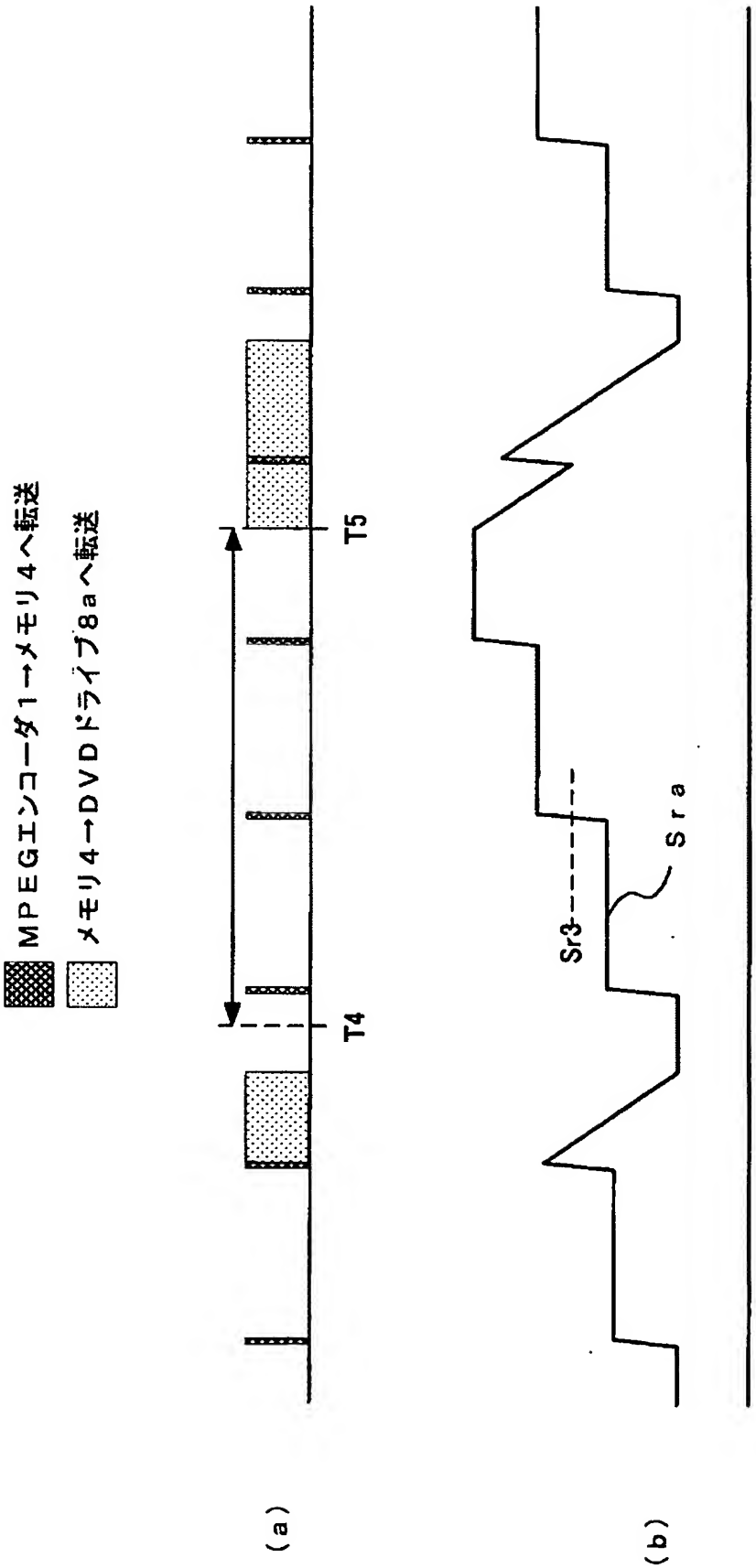
前記暗号復調する必要がないと判断された場合は、前記暗号復調を行わずに、前記蓄積されたディジタル信号を出力し、

前記暗号復調する必要があると判断された場合は、当該判断の時点から前記暗号復調が前記暗号鍵により有効化されるまでの間、すでに蓄積されているディジタル信号を出力し、前記有効化が行われた後で前記暗号化された信号を前記暗号復調して出力するよう制御することを特徴とする暗号復調方法。

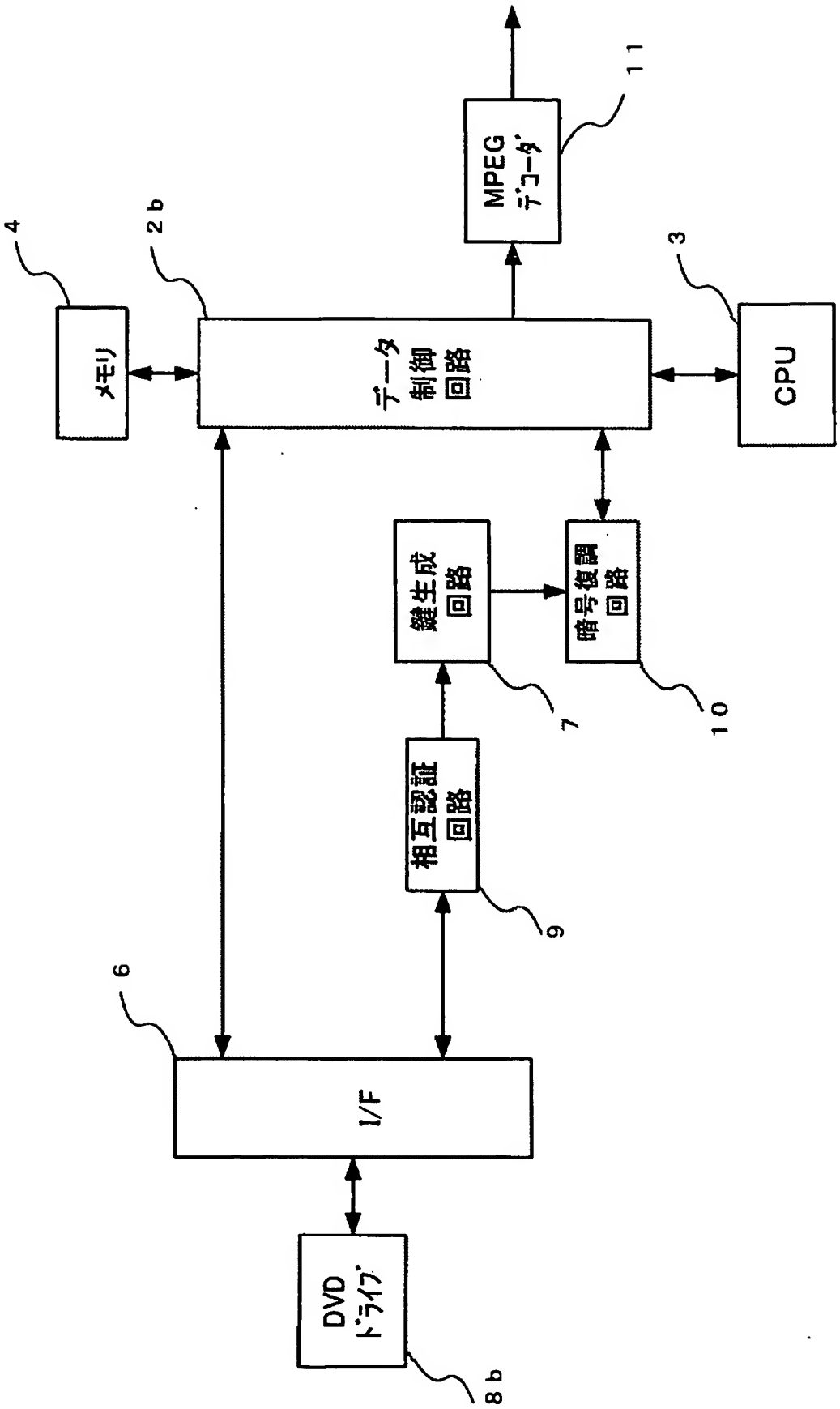
[図1]


1
MPEG エンコーダ
2a
データ制御回路
3
CPU
4
メモリ
5
暗号化回路
7
鍵生成回路
9
相互認証回路
6
I/F
8a
DVD ドライブ

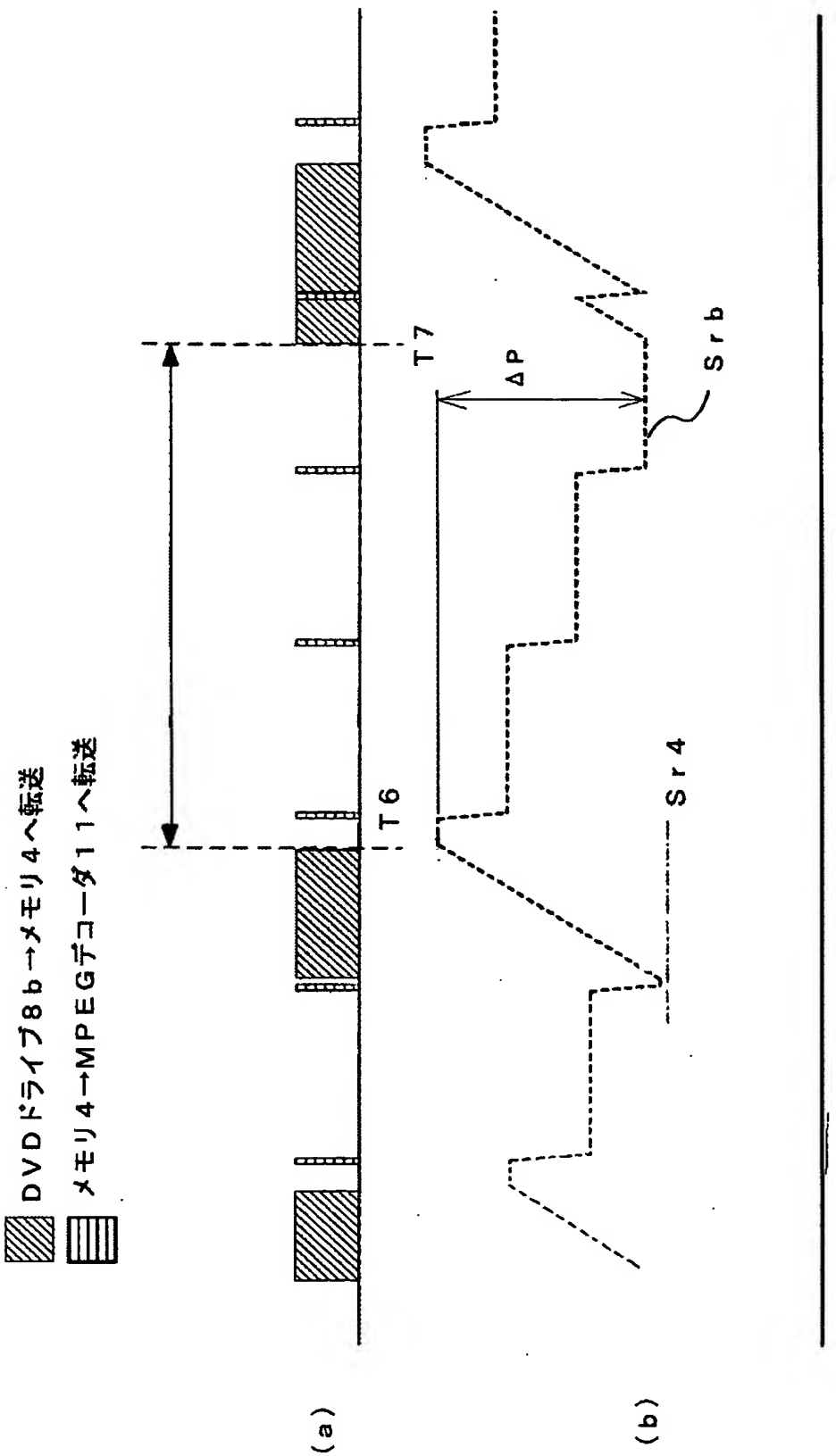
[図2]



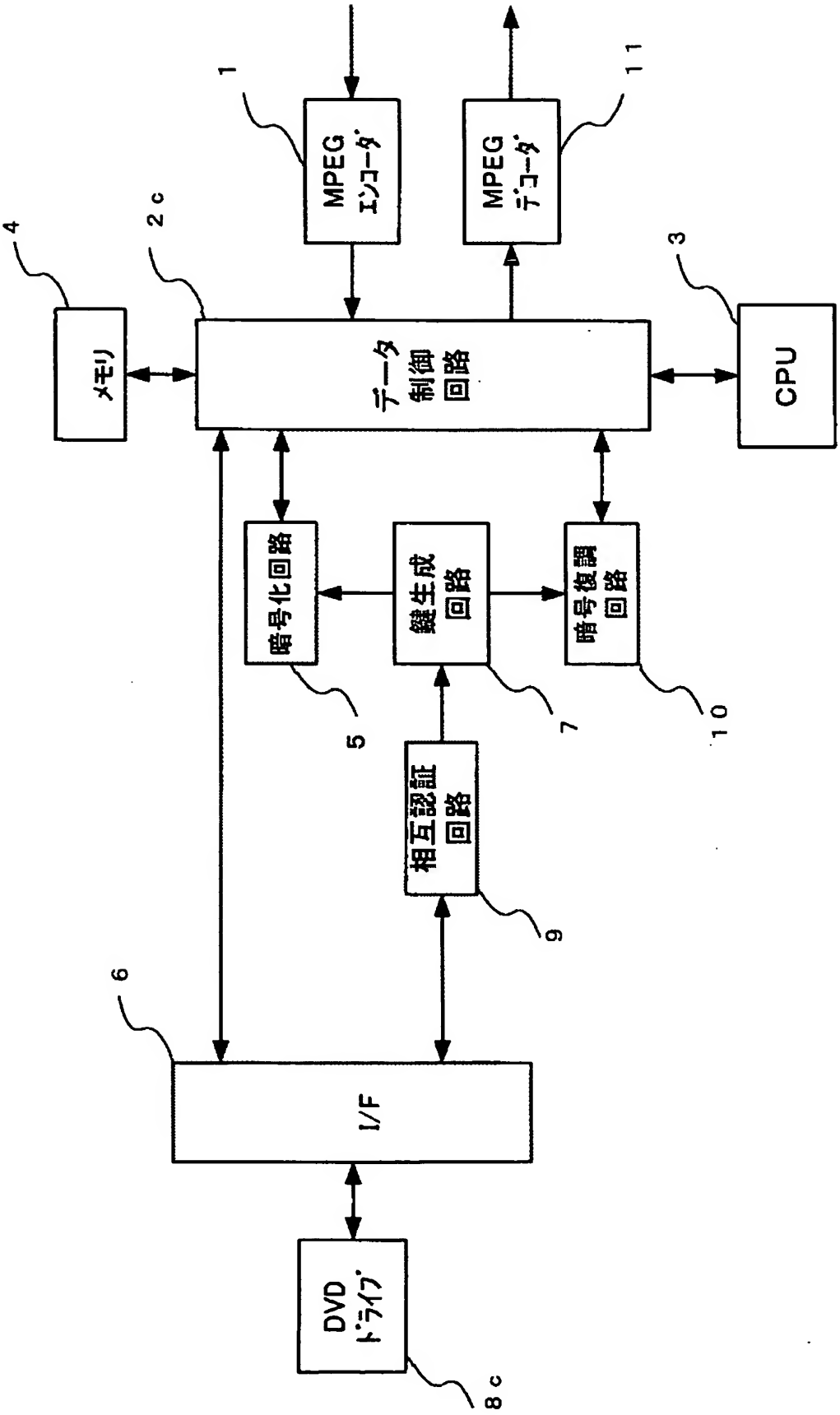
[図3]


MPEG
ﾃﾞｺｰﾀﾞ
11
4
2b
3
メモリ
データ
制御
回路
CPU
鍵生成
回路
暗号復調
回路
7
10
相互認証
回路
9
6
I/F
DVD
ﾄﾞﾗｲﾌﾞ
8b

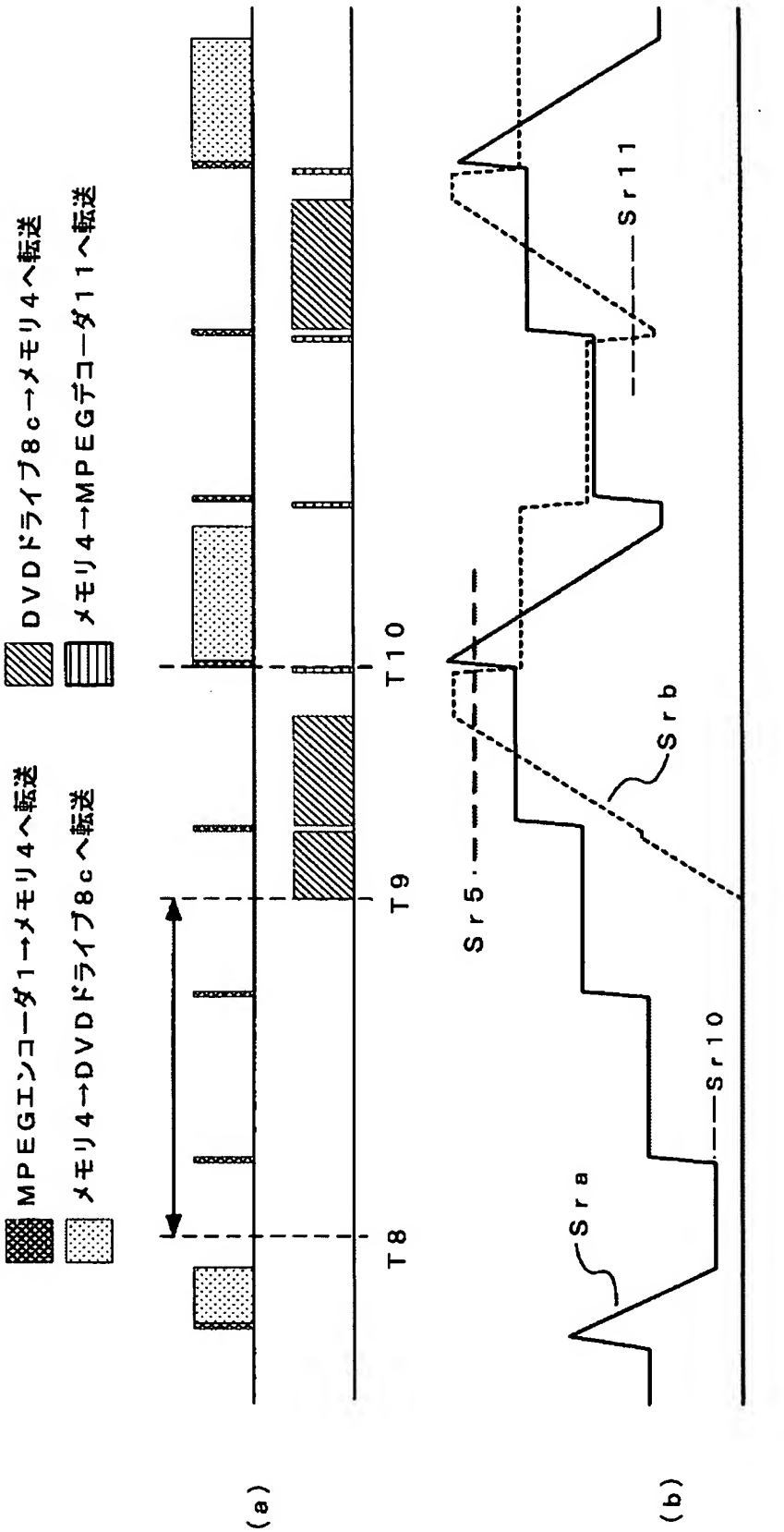
[図4]



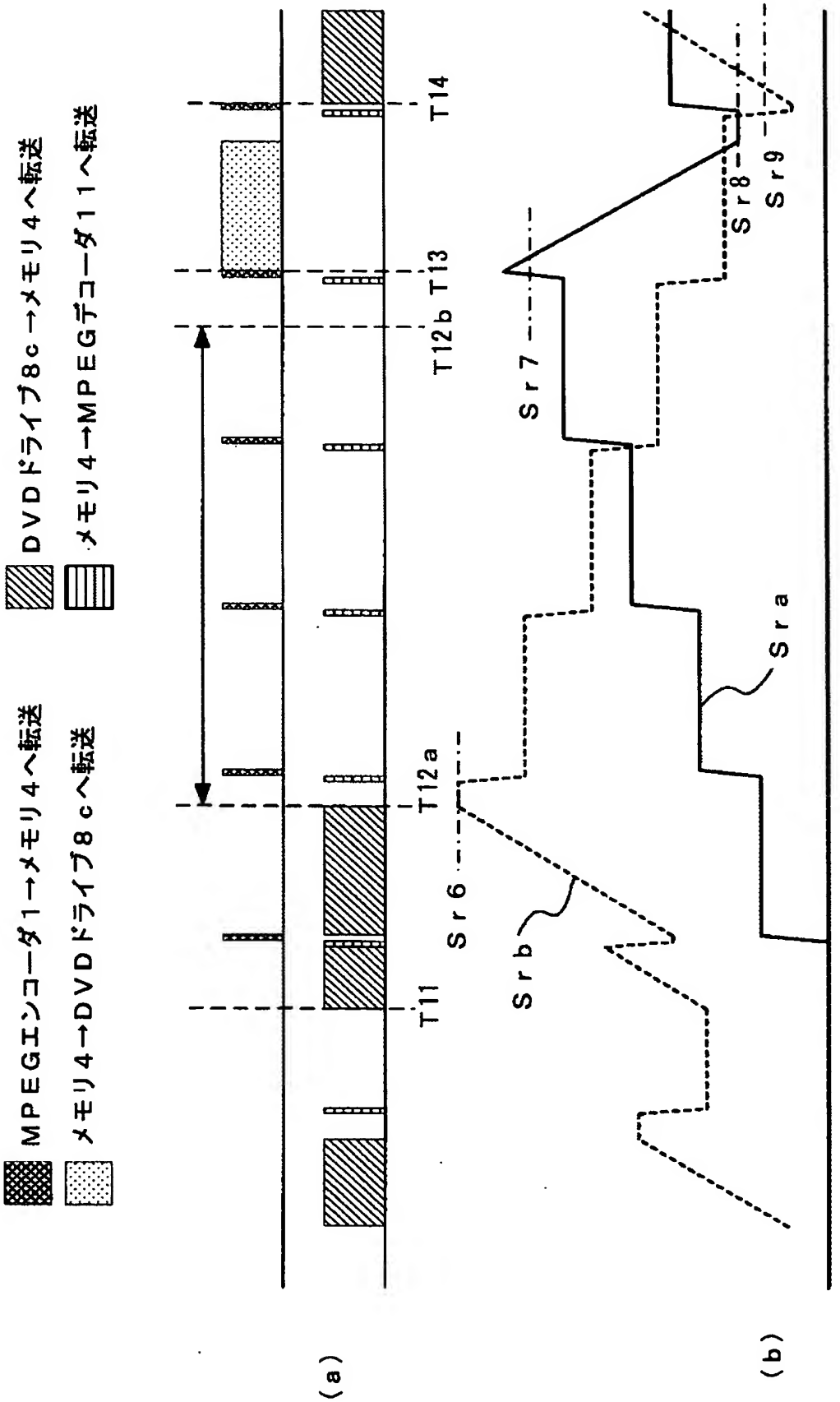
[図5]


1
MPEG エンコーダ
11
MPEG デコーダ
4
メモリ
2c
データ制御回路
3
CPU
暗号化回路
5
鍵生成回路
7
暗号復調回路
10
相互認証回路
9
6
I/F
DVD ドライブ
8c

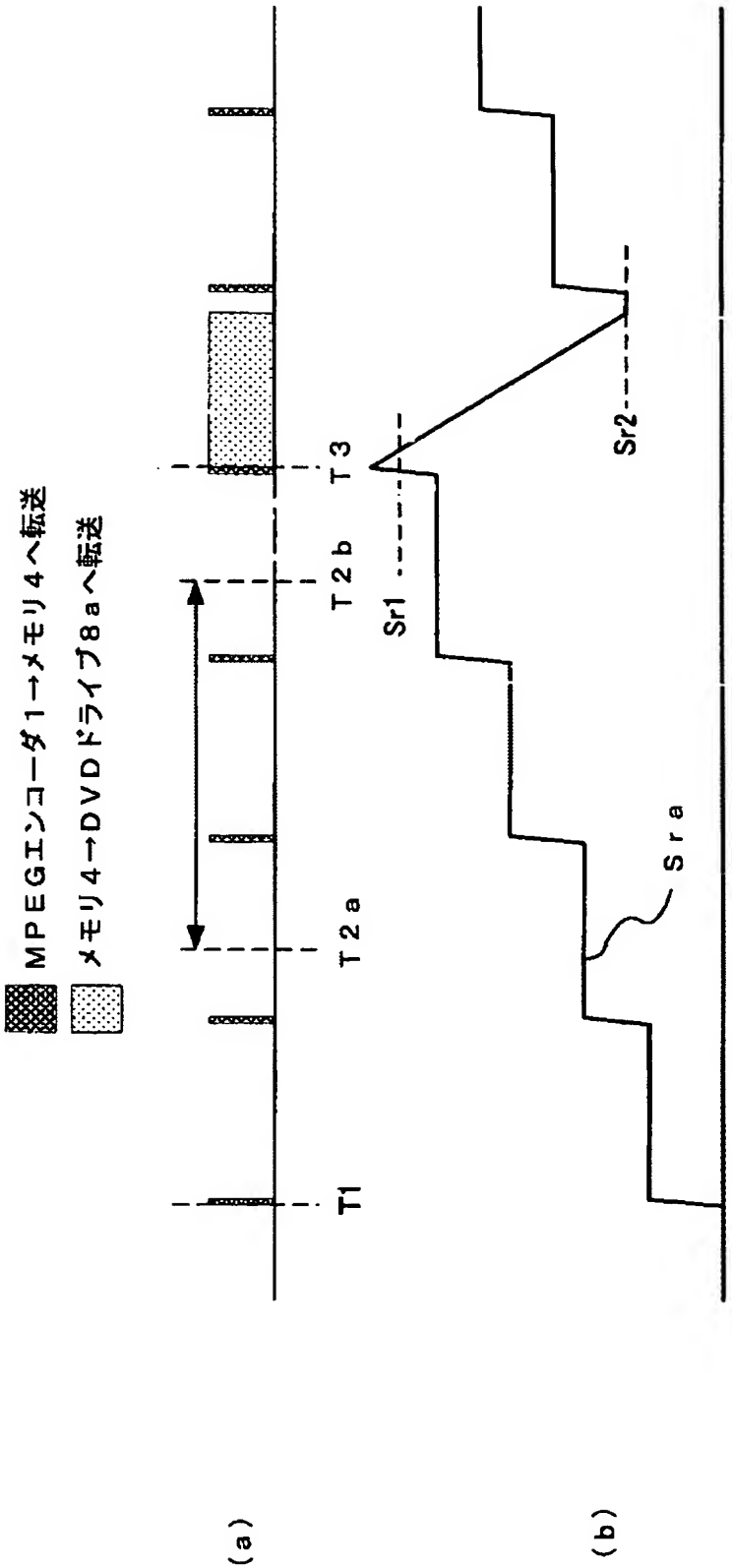
[図6]


MPEGエンコーダ1→メモリ4へ転送
メモリ4→DVDドライブ8cへ転送
DVDドライブ8c→メモリ4へ転送
メモリ4→MPEGデコーダ11へ転送
T8
T9
T10
Sr5
Sra
Srb
Sr10
Sr11
(a)
(b)

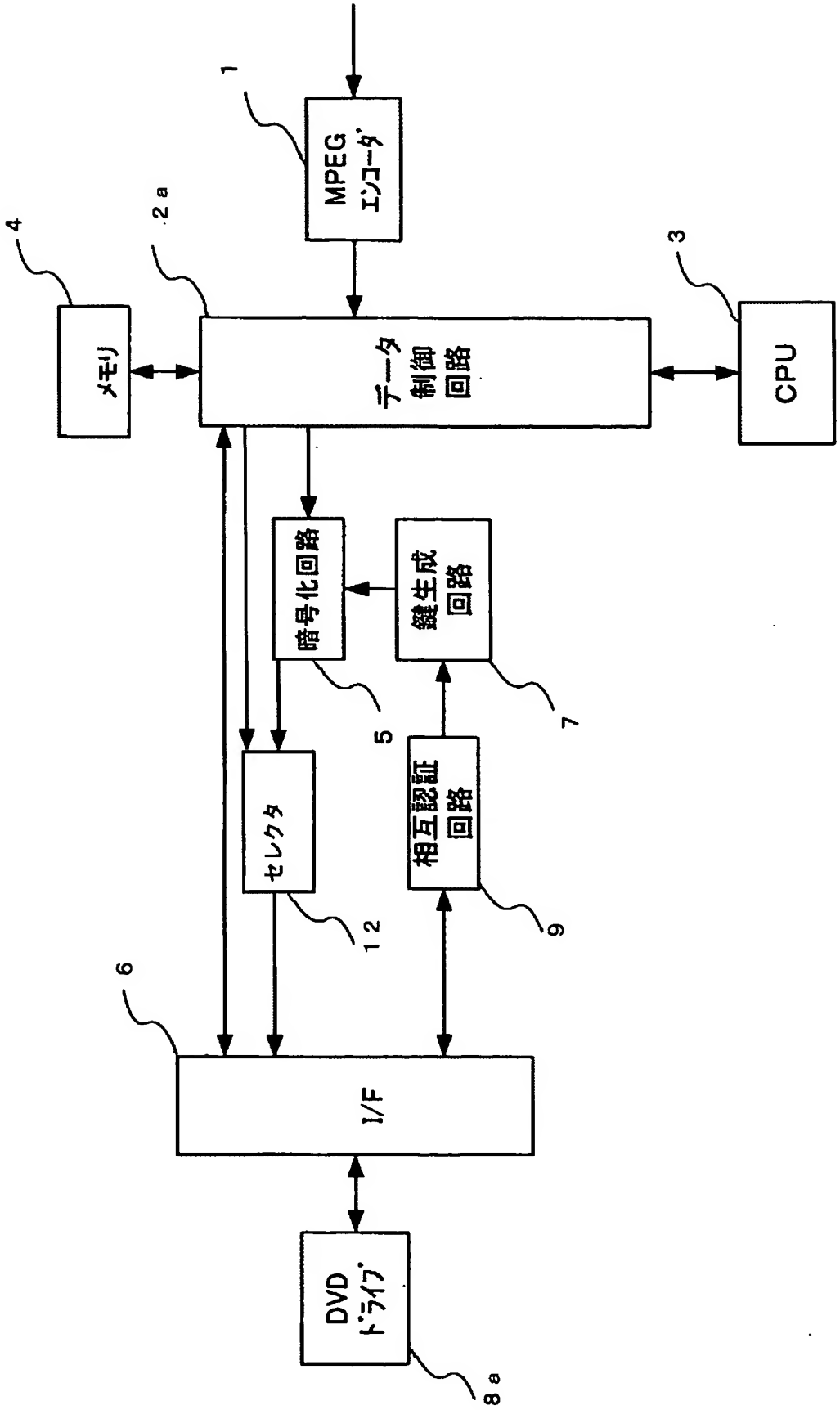
[図7]


MPEGエンコーダ1→メモリ4へ転送
メモリ4→DVDドライブ8cへ転送
DVDドライブ8c→メモリ4へ転送
メモリ4→MPEGデコーダ11へ転送
T11
T12a
T12b
T13
T14
Sr6
Srb
Sr7
Sr8
Sr9
Sra
(a)
(b)

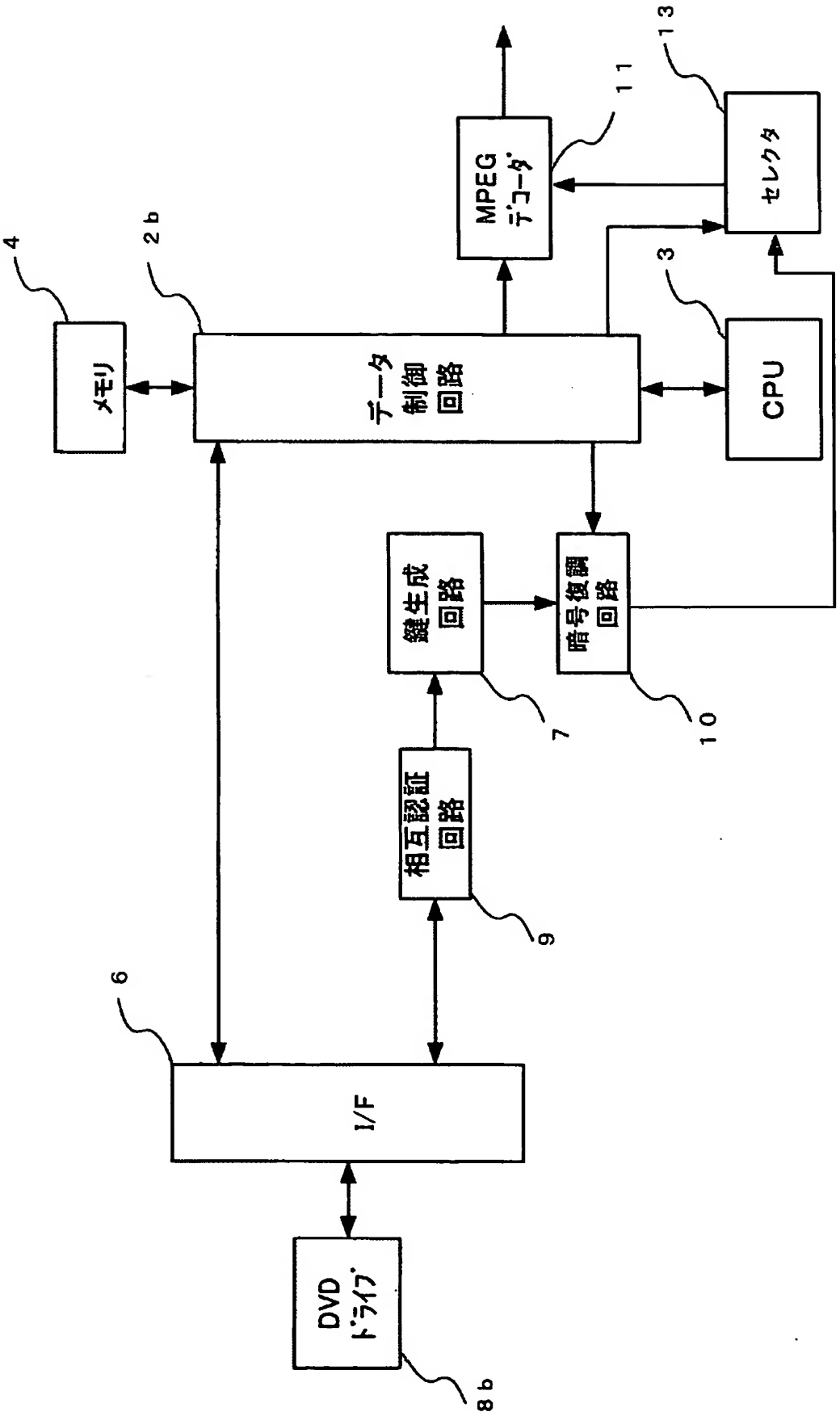
[図8]


MPEGエンコーダ1→メモリ4へ転送
メモリ4→DVDドライブ8aへ転送
T1
T2a
T2b
T3
Sr1
Sr2
Sra
(a)
(b)

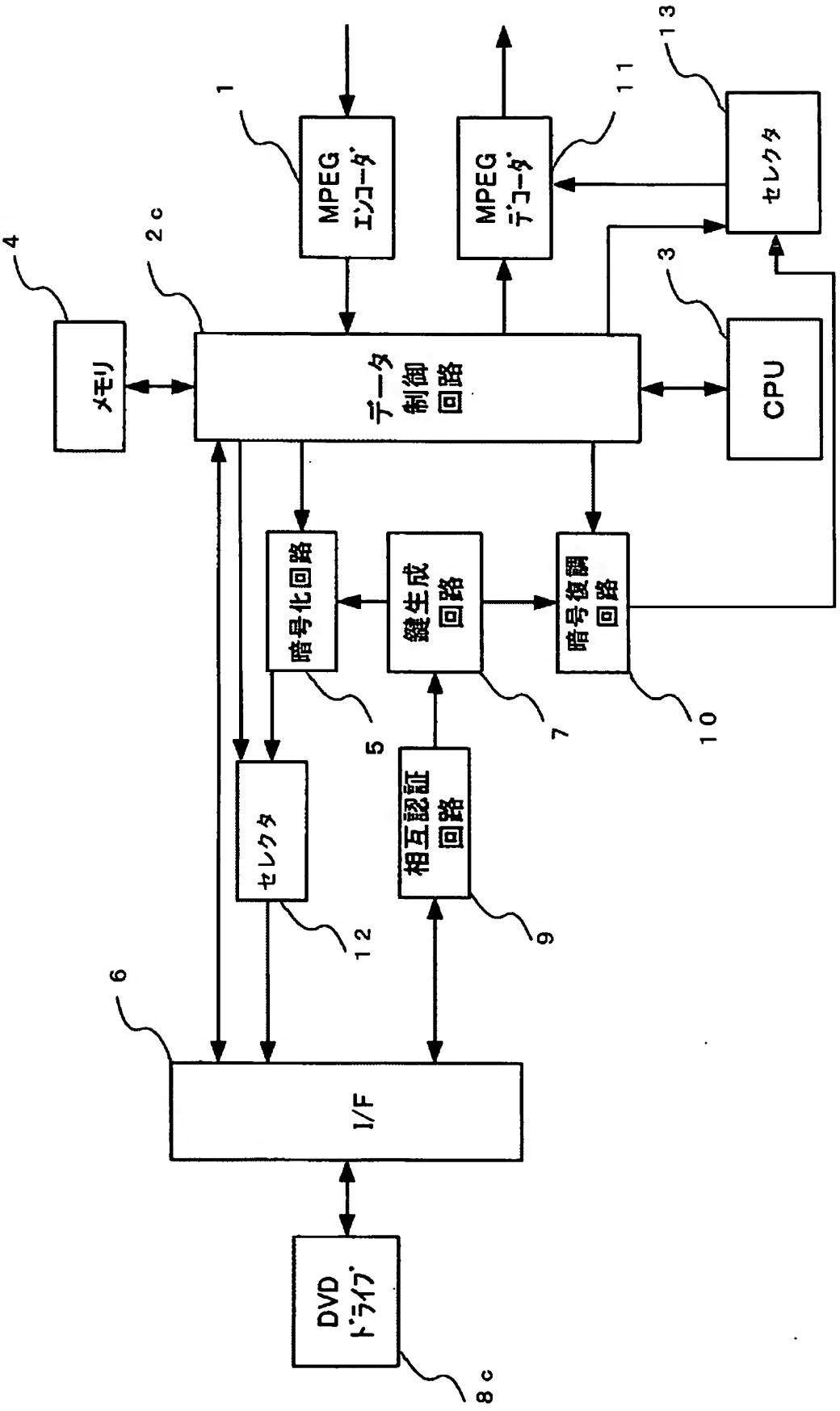
[図9]


1
MPEG
エンコーダ
2a
データ
制御
回路
3
CPU
4
メモリ
暗号化回路
5
鍵生成
回路
7
セレクタ
12
相互認証
回路
9
6
I/F
DVD
ドライブ
8a

[図10]


13
セレクタ
11
MPEG
デコーダ
4
メモリ
2b
データ
制御
回路
3
CPU
鍵生成
回路
7
暗号復調
回路
10
相互認証
回路
9
6
I/F
DVD
ドライブ
8b

[図11]


1
MPEG エンコーダ
11
MPEG デコーダ
13
セレクタ
4
メモリ
2c
データ制御回路
3
CPU
暗号化回路
5
鍵生成回路
7
暗号復調回路
10
セレクタ
12
相互認証回路
9
6
I/F
DVD ドライブ
8c

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/010218

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G11B20/10, G06F12/14, G09C1/00, H04N5/91

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G11B20/10, G11B19/00, G06F12/14, G09C1/00, H04N5/91

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2001-76431 A (Sony Corp.), 23 March, 2001 (23.03.01), Column 11, line 19 to column 12, line 21, column 19, line 8 to column 24, line 3; Figs. 3, 4, 10, 11 & EP 1081699 A1	1-11
Y	JP 2002-64482 A (Matsushita Electric Works, Ltd.), 28 February, 2002 (28.02.02), Column 4, line 25 to column 8, line 31; Figs. 1 to 4 (Family: none)	1,3,4-6,10

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 29 September, 2004 (29.09.04)	Date of mailing of the international search report 19 October, 2004 (19.10.04)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/010218

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 5-257816 A (Fujitsu Ltd.), 08 October, 1993 (08.10.93), Full text; Figs. 1 to 14 & EP 561685 A1 & US 5392351 A & US 5555304 A & US 5796824 A	4-11
Y	JP 2001-77802 A (Sony Corp.), 23 March, 2001 (23.03.01), Column 9, line 40 to column 13, line 27; Figs. 1 to 10 (Family: none)	4-11
Y	JP 2002-344440 A (Toshiba Corp.), 29 November, 2002 (29.11.02), Full text; Figs. 1 to 12 & US 2002/174239 A1	2,3,7-9,11

国際調査報告

国際出願番号 PCT／JP2004／010218

A. 発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷ G11B20／10, G06F12／14, G09C1／00, H04N5／91

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷ G11B20／10, G11B19／00, G06F12／14, G09C1／00, H04N5／91

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2004年
日本国登録実用新案公報	1994－2004年
日本国実用新案登録公報	1996－2004年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 2001－76431 A（ソニー株式会社） 2001．03．23，第11欄第19行～第12欄第21行， 第19欄第8行～第24欄第3行，第3，4，10，11図 & EP 1081699 A1	1－11
Y	JP 2002－64482 A（松下電工株式会社） 2002．02．28，第4欄第25行～第8欄第31行， 第1－4図（ファミリーなし）	1，3，4－6，10

[x] C欄の続きにも文献が列挙されている。

[ ] パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日 29．09．2004	国際調査報告の発送日 19.10.2004
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 早川 卓哉 5Q 9295 電話番号 03－3581－1101 内線 3590

様式PCT／ISA／210（第2ページ）（2004年1月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００４／０１０２１８

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ　５－２５７８１６　Ａ（富士通株式会社） １９９３．１０．０８，全文，第１－１４図 ＆　ＥＰ　５６１６８５　Ａ１ ＆　ＵＳ　５３９２３５１　Ａ ＆　ＵＳ　５５５５３０４　Ａ ＆　ＵＳ　５７９６８２４　Ａ	４－１１
Ｙ	ＪＰ　２００１－７７８０２　Ａ（ソニー株式会社） ２００１．０３．２３，第９欄第４０行～第１３欄第２７行， 第１－１０図（ファミリーなし）	４－１１
Ｙ	ＪＰ　２００２－３４４４４０　Ａ（株式会社東芝） ２００２．１１．２９，全文，第１－１２図 ＆　ＵＳ　２００２／１７４２３９　Ａ１	２，３，７－９，１１